



March 20, 2017

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW, Room TWA325
Washington, DC 20554

Re: National Emergency Address Database Privacy and Security Plan PS Docket No. 07-114

Dear Ms. Dortch:

The Center for Democracy & Technology is a nonprofit advocacy organization that works to shape technology policy and architecture to focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy, promote security, and advance democratic values.

CDT recognizes the tremendous positive impact that better 911 location accuracy may have for public safety and appreciates the opportunity to comment on the National Emergency Address Database (NEAD) Privacy and Security Plan. In January 2015, CDT joined with other public advocacy organizations to express concerns about the privacy impact of the NEAD.¹ We cautioned that users of networked devices likely do not expect that information about their personal devices and physical address will be stored in a national database that is accessible to multiple parties. In those comments, we offered several recommendations for protecting user privacy including strong limits on third-party access to the database and opt-out mechanisms for individuals.

CDT is pleased that the draft NEAD Privacy and Security Plan appears largely to address these concerns. We write now to highlight several aspects of the NEAD Platform that protect privacy and security, and suggest how the plan's practices might evolve in the future:

1. **The NEAD Platform is supported by a draft security plan that mandates strong security controls.** As drafted, the NEAD security plan includes specific technical requirements for encrypting information both in transit and at rest in the NEAD, routine penetration testing, and maintaining secure operating systems and applications on the NEAD Platform. The plan also provides for access controls, personnel training, and ongoing monitoring. These through implementation of these policies and controls will be critical for maintaining the public's trust in the NEAD. Location information is highly sensitive, and as the NEAD Platform expands nationwide, this database of location information will present an increasingly alluring target for malicious agents. We note that the expansion of the NEAD Platform over time will require an ongoing commitment to comprehensive data security measures and may require additional financial and technical investments by wireless carriers and the NEAD Platform.

¹ Privacy Advocates' Letter to Marlene H. Dortch, Secretary, FCC (Jan. 22, 2015), <https://ecfsapi.fcc.gov/file/60001015769.pdf>.

2. **Limits to the collection and processing of personal information.** As described in the plan, the NEAD Platform is not designed to store information about any identifiable individuals but rather is a database only of verified wireless access points that are mapped to 911-dispatchable addresses. During a 911 call, wireless carriers provide the NEAD Platform only with the MAC addresses of detected wireless access points to compare against the database. These limitations mitigate the potential usefulness of the NEAD Platform as a potential surveillance tool by law enforcement or other government agencies. We were also pleased to see that the draft privacy plan continues efforts to impose a blanket restriction on the use of the NEAD Platform for any commercial purpose. Ensuring the accuracy and effectiveness of 911 services is an important goal to improve public safety, but so is maintaining public trust in the Platform: the careful coordination and resources devoted to the NEAD Platform by wireless carriers must not be used as a backdoor to advance the sharing or selling of information for reasons other than providing emergency services.
3. **CDT recognizes that the NEAD Platform remains a work-in-progress.** It will likely be many years yet before the full functionality of the NEAD Platform is available for 911 services across the United States, and it is apparent from the draft privacy and security plan that development of the NEAD Platform will occur in stages. Specifically, we note that information about wireless access points in the NEAD Platform will be provided not only by wireless carriers but also (1) other entities, including building managers and major businesses, and eventually (2) individual consumers. Properly incentivizing these contributions will require an ongoing commitment by the NEAD Platform to respect the privacy of individuals. This will require much more robust engagement with the public by the NEAD, which presently has no public-facing website or online presence.² The NEAD should develop educational materials and a method for the public to submit their questions and concerns beyond formal comments such as these. As the service develops, individuals should also be offered information and clear choices about how they can add, access, update, or remove their personal information and information they contribute regarding wireless access points.

CDT is broadly supportive of the draft privacy and security plan proposed by the NEAD Platform. It is a strong foundation, and we expect that the NEAD Platform will continue to engage with consumer advocates and privacy and technology experts as the Platform evolves.

Thank you for this opportunity to share our comments on the draft plan, and please let us know if you have any questions.

Sincerely,
Joseph Jerome
Policy Counsel, CDT

² See <http://www.911nead.org/> (last visited Mar. 19, 2017).